

Amendments to the Drawings:

The attached sheets of drawings include proposed changes to Figs 1 and 2b.

REMARKS

Applicant respectfully requests reconsideration of this application as amended.

Attached hereto is a substitute Declaration that overcomes the objection to the Declaration. Furthermore, attached hereto is a marked-up version of Figure 1 and Figure 2B with the requested elements identified by English language legends. The Examiner is kindly requested to approve Applicant's proposed drawing corrections.

Attached hereto is an Abstract in compliance with MPEP 608.01(b). The specification has also been amended to include a brief description of Fig. 4c.

Regarding the objection to Claims 7 and 12, as well as the rejection of Claims 7-12 under 35 U.S.C. § 112, Applicant has amended the specification to clarify that the key diversification process implemented in step 1003, as represented in Fig. 3, can be a process supported by an algorithm known as zero knowledge signature mechanisms which can be readily implemented as a FIAT-SHAMIR or GUILLOU QUISQUATER algorithm, both of which are usable for this purpose. The GUILLOU QUISQUATER algorithms are also known as the GQ algorithm and are well known in the field. For example, a summary of these algorithms can be found in Applied Cryptography, Second Edition, by Bruce Schneier, John Wiley and Sons, 1996.

More particularly, these algorithms are known as identity-based signature scheme or identity-band zero-knowledge mechanisms in the art. An identity-based zero knowledge mechanism can be readily implemented using the FIAT-SHAMIR or GUILLOU QUISQUATER algorithms. The concept was invented in 1984 by A. Shamir (A. Shamir, Identity Based Cryptosystems and Signature Schemes, Advances in Cryptography-Crypto'84, LNCS 196, pp. 47-53, Springer, 1994). The FIAT-SHAMIR scheme can be used for digital signatures. In this case, it is called the FEIGE-FIAT-SHAMIR signature scheme (U. Fiege, A. Fiat, A. Shamir, Zero-Knowledge Proofs of Identity, Journaled Cryptography, Vol. 1, No. 2, pp. 77-95, 1998). In the same way, the GUILLOU QUISQUATER scheme can be used to digitally sign as shown in, for example, the article by Louis C. Guillou and John-Jacque Quisquater, A Paradoxical Identity-Based Signature Scheme Resulting From Zero-Knowledge, S. Goldwasser, Editor, Crypto '1988, Vol. 403 of LNCS, pp. 216-231, Springer-Berlag, August 1989.

Should the Examiner deem it necessary, copies of this documentation can be supplied upon request.

The specification has further been amended to correct typographical errors as identified by the Examiner. In particular, Applicant would like to thank the Examiner for the errors pointed out in paragraphs 5-6 of the Office Action and fully agree that the public key sent to the CA to be certified is the public key K_p of the asymmetric key pair. Appropriate corrections have been made.

Regarding the art-based rejections, the claims are rejected in view of various combinations of Matyas, Pauschinger, Austin, Yuval, Multerer, Menezes, and Holloway. As agreed by the Examiner, Matyas does not disclose associating an identification code of an authorized operator with the onboard system, or that the private authentication key is a diversified private key, that the diversified private key is generated from a mother private key and the device ID. However, the Office Action points to the various other supplemental references for these teachings.

Claim 7 recites, *inter alia*,

A method for verifying the usage of public keys of a set of asymmetric keys, a public key (K_p) and private key (K_s) generated for a given use, such as encryption/decryption or digital signature verification/generation, by an on-board system and stored in the storage area of the on-board system (S_i) equipped with cryptographic calculation means and externally accessible read/write-protected means for storing digital data, said digital data (ID_{di}) comprising at least a serial number (SN_i) for identifying the on-board system and an identification code (OP_j) of an operator authorized to configure said on-board system, a request being formulated by said on-board system by transmitting a request message (MRCA) containing said public key (K_p) to a certification authority (CA), comprising:

PRIOR TO ANY TRANSMISSION OF A CERTIFICATION REQUEST, DURING THE CONFIGURATION OF A SET (L_k) OF ON-BOARD SYSTEMS (S_i) BY THE AUTHORIZED OPERATOR:

- generating by the authorized operator, for said set of on-board systems, a mother public key (K_{pM}) and a mother private key (K_{sM}) used in connection with a process supported by an algorithm ($CA1M$);
 - publishing said mother public key (K_{pM}) associated with the algorithm ($CA1M$), the identification code of said authorized operator (OP_j), and defining a range of on-board system identifiers for the set (L_k) of on-board systems;
 - calculating, for each on-board system of said set (L_k) of on-board systems, from said mother private key (K_{sM}) and from the serial number (SN_i) of the on-board system, a diversified private key (K_{sMi}), and storing said diversified private key (K_{sMi}) in said externally accessible, read/write-protected storage area, and;
- PRIOR TO ANY TRANSMISSION OF A CERTIFICATION REQUEST MESSAGE:**

- generating by the on-board system a certification request (RCA) containing, in particular, a field of the public key (Kp) and usage indicators (U) of said public key,
- using said calculation means and said diversified key (KsMi) associated with this on-board system to calculate a cryptographic control value (Sci) on the entire request (RCA), said cryptographic control value being a digital signature calculated by means of the diversified private key (KsMi);

WHEN A CERTIFICATION REQUEST IS SENT TO THE CERTIFICATION AUTHORITY BY THE ON-BOARD SYSTEM:

- forming a certification request message (MRCA) containing the request (RCA), the identifier (IDdi) of the on-board system, the request message being constituted by the identification code (OPj) of this authorized operator and by the serial number (SNi) of the on-board system, and a cryptographic control value (Sci);
 - transmitting to the certification authority (CA) said request message (MRCA) formed during the preceding phase and containing the public key (Kp) and the usage indicators (U) subject to said certification, and said cryptographic control value (Sci);
- and

WHEN A CERTIFICATION REQUEST MESSAGE (MRCA) IS RECEIVED BY THE CERTIFICATION AUTHORITY:

- retrieving the identification code of the authorized operator (OPj) from the digital data (IDdi) of the on-board system,
- retrieving, from said identification code (OPj) of said authorized operator, the value of the mother public key (KpM) as well as the identifier of the algorithm (CA1M) associated with the set (Lk) of the on-board system,
- verifying, from said mother public key (KpM), from said serial number (SNi) of the on-board system, and from said certification request message (MRCA) received, said cryptographic control value (Sci), and establishing the authenticity of said cryptographic control value and the source of this certification request.

In contrast, none of the cited references teach or suggest all of the specific steps of Claim 7. For example, none of the cited references teach that prior to any transmission of a certification request, during a configuration of a set of on-board systems by the authorized operator, the generating, publishing, calculating, generating and using steps as claimed.

Furthermore, upon a certification request being sent to the certification authority by the on-board system, forming, transmitting steps are performed and when the certification request message is received by the certification authority, retrieving and verifying steps are performed. Applicant respectfully submits there is no teaching or suggestion of these steps in the cited references.

Furthermore, Matyas is directed toward a data processing network including data processors coupled to each other to enforce a network cryptographic system comprising a certification system. Once the network

security policy is encoded in a configuration vector in device A, this is sent to device B to be decoded and implemented in device B. Matyas does not disclose or suggest the features of Claim 7 in that 1) the cryptographic facility of Matyas does not and can not be equated with the storage area of an on-board system as claimed; 2) Matyas fails to teach or suggest any capability directed to storage of digital data comprising at least a serial number for identifying the on-board system and an ID code of an operator authorized to configure the on-board system. In contrast, the manufacturer's identification number relied upon by the Office cannot be considered to be an identification code of an authorized operator as claimed.

Pauschinger is directed toward a method for operating a postage meter machine for the generation of a security imprint having a signature on a piece of mail by generating a pair of keys, storing the keys in a device, storing a public read key in a certificate in memory allocated to a postage machine identifier, and formatting the machine readable information to be printed by a printer, which will include a digital signature and unencrypted information. Pauschinger fails to overcome the deficiencies as noted above in relation to Matyas. Moreover, there is nothing in Pauschinger's postage meter machine or its database that can be equated to associating the identification code of an authorized operator with the onboard-system as claimed.

Austin is relied on for supplying the recognized deficiency of Matyas in that Matyas does not disclose that the private authentication key is a diversified key. Austin features a method of generating key values for use in smart cards such as credit card transactions. The generation by the parent entity, e.g., the trust identity, of public key values N_e where N is the product of first and second prime number P, Q . However, Austin fails to overcome the recognized deficiencies of Matyas in that Austin as well does not teach or suggest the use of diversified private keys. Moreover, Matyas uses an RSA algorithm which does not belong to the class of zero-knowledge algorithms as claimed.

Yuval is relied on as disclosing that the diversified private key is generated from a mother private key and the device ID. Motivation for combining Matyas and Yuval is stated as being that the "software encrypted using

a single encryption key could be decrypted using multiple encryption keys, each of which is unique to a particular user.” Yuval is directed toward distributing software by controlling unauthorized access to the data. Yuval explains that the multiplicity of “decryption keys” are the products of the numeric representations of identifying information related to users and the unique user keys generated using the numeric representations and the “true” decryption key. Therefore, a particular user will have both a unique user key and a numeric representation.

However, as recited in Claim 7, a diversified private key is calculated from the mother private key and the serial number of the on-board system, for each on-board system of a set of on-board systems stores the private key in the externally accessible, read/write-protected memory. This feature is simply not taught in any of the cited references. Moreover, Applicant respectfully submits that the motivation to combine the teachings of Yuval and Matyas is defective in that software using multiple decryption keys does not provide any motivation to arrive at a calculation step of the diversified private key derived from the mother private key and the serial number. Moreover, there is no user entry and the fact that Matyas uses an RSA algorithm which does not belong to the class of zero-knowledge algorithms reinforces the non-combinability of the references.

The remaining references, taken either alone or in combination, also fail to overcome the deficiencies as noted above in relation to Matyas, Pauschinger, and Austin.

The application is thus in condition for allowance. A prompt and favorable Notice of Allowance is respectfully requested.

Should the Examiner believe anything further is desirable in order to place the application in even better condition for allowance, the Examiner is encouraged to contact Applicant’s representative at the telephone number listed below for the scheduling of a personal interview.

The Commissioner is hereby authorized to charge to deposit account number 50-1165 (T3370-906620) any fees under 37 CFR § 1.16 and 1.17 that may be required by this paper and to credit any overpayment to that Account. If any extension of time

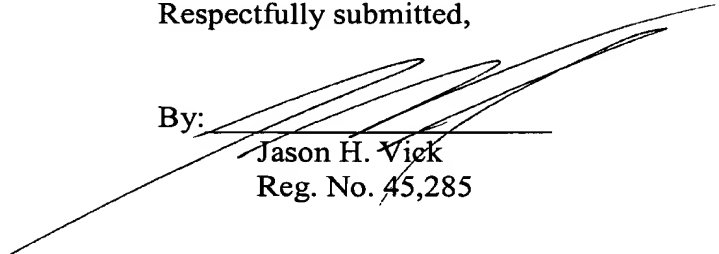
is required in connection with the filing of this paper and has not been separately requested, such extension is hereby requested.

Respectfully submitted,

JHV:jab

Miles & Stockbridge P.C.
1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102-3833
(703) 903-9000

By:



Jason H. Vick
Reg. No. 45,285

January 31, 2005